



PATENT APPLICATION
ATTORNEY DOCKET: 10624.0015

Patent Application of:

Group Art Unit: 2766

MARCEL M. YUNG *ET AL*

Examiner: C. Tucker

Serial No.: 09/429,624

Filed: October 29, 1999

Date: April 2, 2001

For: INCORPORATING SHARED
RANDOMNESS INTO DISTRIBUTED
CRYPTOGRAPHY

#8 /
A
B#
4-18-01

Only
Claims
Added
RECEIVED
APR-9 2001
TC 2100 MAILROOM

RESPONSE

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

This is a reply to the Office communication dated October 3, 2000 ("the pending Action") in the above-identified application ("the pending Application").

AMENDMENTS

Please amend the pending Application as follows.

IN THE CLAIMS:

Please amend the following claims as set forth below:

- (N.E.)
Mark-up
Copy not
included.
1. A method of distributed cryptographic computation using a plurality of distributed electronic devices, said method comprising:
 - (a) computing shared values over a known and agreed context;
 - (b) generating random values using said shared values;

04/05/2001 TBESHAH1 00000078 09429624

01 FC:103

36.00 OP